IJES
15,2

Received 2 June 2025
Revised 3 October 2025
23 December 2025
Accepted 14 January 2026

Paradox of cybersecurity? The democratic deficit in municipal work to raise citizens' risk awareness

Gabriella Sandstig
Department of Journalism, Media and Communication, University of Gothenburg, Gothenburg, Sweden
Max Boholm
School of Public Administration, University of Gothenburg, Gothenburg, Sweden, and
Johan Berlin
Department of Social and Behavioural Studies, University West, Trollhättan, Sweden and
School of Public Administration, University of Gothenburg, Gothenburg, Sweden

Abstract

Purpose – The increased dependence on information technology for storage, access and analysis of information has increased the vulnerability of states, organisations and individuals in the last decade. Despite cyberattacks being one of the major risks perceived by citizens, little research has addressed how the public sector at local level is managing the challenges that raising society's preparedness in relation to cyber threats entails. The aim of this study is therefore to analyse the extent to which municipalities are taking measures to increase citizens' awareness of information and cybersecurity risks and to discuss why potential challenges might arise.

Design/methodology/approach – A cross-sectional survey was used by the Swedish Association of Local Authorities and Regions (SALAR) to collect data from 234 of Sweden's 290 municipalities in the period 10/3-25/4 2023.

Findings – The results show that 81% of the municipalities are not engaged in raising citizens' awareness of information and cybersecurity risks, and that established working procedures for information and cybersecurity are relevant in understanding this lack of engagement. Interpretive insight from previous literature also shows the relevance of the range of professional logics, which does not provide sufficient incentives for the profession engaged in planning and managing the information and cyber risks to cooperate.

Originality/value – The paper addresses the citizen perspective in relation to work carried out on information and cybersecurity risks at the municipal level. The article's contribution is to show that the citizen's perspective does not have any prominence in the work that municipalities conduct on information and cybersecurity risks.

Keywords Information security, Cybersecurity, Risk communication, Municipalities, Citizen engagement

Paper type Research article

Introduction

Questions about cybersecurity, i.e. how to protect digital information and information systems, as well as their users, from various threats (cf. ENISA, 2015; von Solms and van Niekerk, 2013), are high on the agendas of public organisations, local authorities and nation states

Funding details: The authors gratefully acknowledge the financial support provided by the Swedish Research Council (Vetenskapsrådet) (Grant/Award Numbers: 2021-06310 and 2022-05405).

Disclosure statement: No potential conflict of interest was reported by the authors.

International Journal of Emergency Services
Vol. 15 No. 2, 2026
pp. 178-196
Emerald Publishing Limited
e-ISSN: 2047-0908
p-ISSN: 2047-0894
DOI 10.1108/IJES-05-2025-0029

(Backman, 2021; Preis and Susskind, 2022; Sandstig, 2025) [1]. However, public authorities' preparedness for cyber threats is documented to be at a low level (Preis and Susskind, 2022; Andreasson *et al.*, 2024). Some research has been conducted into how to strengthen cybersecurity, with the consequences of cyber crises from a technical or defence perspective often researched at national level (Backman, 2021; Dunn Cavelty, 2025). This while the local government level for the most part is under-explored (Preis and Susskind, 2022).

Most studies of cybersecurity in local government focus on the United States (Norris *et al.*, 2023; Hossain *et al.*, 2025), with more limited research addressing the European context, Germany, for example (Wirtz and Weyer, 2017). This literature consistently finds that municipalities are facing persistent cyber threats but often lack the capacity to manage them effectively. Efforts to strengthen cybersecurity are further complicated by competing priorities as security objectives do not always align easily with values of transparency and openness (Macmanus *et al.*, 2012; Caldarulo *et al.*, 2024). At the same time, insights drawn from specific political and administrative systems cannot be transposed uncritically across countries or time periods, nor related to previous findings. For example, the COVID-19 pandemic and the war in Ukraine have heightened the need for cybersecurity in public organisations, driven by an accelerated reliance on digital technologies and an increase in security threats (Andreasson *et al.*, 2024). Despite the rapid changes in the field, we argue that some previous insights still remain broadly relevant. Municipalities in both the USA and Europe are political and bureaucratic institutions confronted with the complex task of managing cybersecurity under conditions of limited capacity and resources, and with competing institutional demands.

Numerous questions remain to be answered on how municipalities engage with cybersecurity issues. Given the societal consequences of inadequate cybersecurity, it is important to study how the public sector at the local level is managing challenges in raising society's preparedness in relation to cyber threats (Norris *et al.*, 2019; Hatcher *et al.*, 2020). Revealing how municipalities are dealing with cybersecurity will enable it to be managed more effectively in practice (Preis and Susskind, 2022).

Along with the issue of what municipalities are doing to enhance the security of their organisations, an important question is what work they are doing in relation to the security of citizens. A lack of awareness of information and cyber threats means that there is a risk of exposure to unnecessary vulnerabilities both within the organisation as well as in relation to the citizens. For example, previous studies have shown that risk awareness within organisations has positive effects on security (Bulgurcu *et al.*, 2010). And, that citizens' awareness of cybersecurity risks is beneficial in authorities' communication with citizens in times of crisis (Backman, 2021). It is therefore important to examine how and to what extent municipalities engage in protecting their citizens from cyber-related threats (Frandell and Freeney, 2022). Raising public preparedness requires knowledge about how, if at all, municipalities communicate risks to citizens (Boholm, 2019; Graham *et al.*, 2015; Sutton *et al.*, 2015).

> The aim of this study is therefore to analyse the extent to which municipalities are working to increase citizens' awareness of information and cybersecurity risks and to discuss why potential challenges might arise.

For local authorities, there is a tension here between conflicting demands (Macmanus *et al.*, 2012; Caldarulo *et al.*, 2022). On the one hand, the demands for openness and transparency, expected from enlightened and engaged citizens. And on the other hand, the demands from within to protect sensitive information and data (Macmanus *et al.*, 2012; Caldarulo *et al.*, 2022). The local authorities need to manage this inherent challenge, which is growing as the dependence on digital tools increases (Backman, 2021; Chodakowska *et al.*, 2022).

Case of Sweden as a critical case

The case studied here is assumed to be transferable to municipalities in other European countries. As in several European countries (Fuchs *et al.*, 2012), risk and vulnerability

assessments (RVA) are an integrated part of municipalities' public risk communication (Rabe *et al.*, 2024). Furthermore, as Sweden is one of the most transparent countries in the world, Swedish municipalities have highly beneficial conditions for promoting transparency and openness in public activities (Hood and Heald, 2006; Roberts, 2006; Lidberg, 2009; Transparency International, 2024). If the citizens' perspective is not taken into account in Sweden, it is reasonable to assume that the perspective is not a priority in other countries' public activities either. The study can therefore be regarded as a critical case.

Citizen perspective in risk and crisis communication

Risk communication

Risk communication is in this paper defined as part of a social process, a democratic dialogue: "Risk communication is an interactive process of exchange of information and opinion among individuals, groups and institutions. It involves multiple messages about the nature of risk and other messages, not strictly about risk, that express concerns, opinions or reactions to risk messages or to legal and institutional arrangements for risk management" (NRC, 1989:21).

The reasons for communicating risks can be several. To inform or educate to fill a presumed knowledge gap among citizens (Fischhoff, 1995). Here to raise risk awareness, for example, around cybersecurity risks, which in turn facilitates communicating recommendations in a crisis situation (Backman, 2021). Also, to encourage preparations and protective actions by changing, reinforcing or discouraging certain behaviour (Covello *et al.*, 1986). Or to warn and disseminate emergency information (Covello *et al.*, 1986). Risk communication can also be used to invite citizens to participate in solving common problems and conflicts, for example, in environmental, health or security issues (Covello *et al.*, 1986).

Similarities and differences between risk and crisis communication

Similarly, to risk communication, crisis communication is defined by the diversity of communicators involved as well as the instrumental and functional elements of communication during a crisis: "Crisis communication could simply put be understood as the ongoing process of creating shared meaning among and between groups, communities, individuals and agencies, within the ecological context of a crisis, for the purpose of preparing for and reducing, limiting and responding to threats and harm." (Sellnow and Seeger, 2013:13). In this paper, risk communication mainly differs from crisis communication in that it needs to motivate citizens to take preventive measures (Covello *et al.*, 1986). This is because, unlike crises, the threats associated with risks have not yet become manifest and may not be perceived as relevant.

Citizen perspective

The citizen perspective in relation to risk- and crisis communication focuses on the importance of communication for the public (Johansson *et al.*, 2023; Odén *et al.*, 2016). Central themes are how the public and specific groups within it react, communicate and act in terms of risk and crisis situations but also what democratic consequences risk- and crisis communication can entail (Johansson *et al.*, 2023; Odén *et al.*, 2016). The communication is based on ethical considerations of how the public should be able to make informed choices (Sellnow and Seeger, 2013). Free access to information is therefore relevant in relation to the communication of risks during crises (Sellnow *et al.*, 2009; Sellnow and Seeger, 2013). When we make an ethical assessment, we evaluate whether a behaviour or a decision is right or wrong, good or bad. Municipalities have a specific responsibility to communicate risks to relevant stakeholders and produce reliable and relevant information (Rabe *et al.*, 2024). The citizen perspective thus represents the enlightened citizen in a democratic society who makes informed choices based on ethical considerations. The choice can affect citizens' future and ultimately enable them to be better prepared to manage crises (Sellnow and Seeger, 2013).

Broadening the citizen perspective with vulnerable groups

However, broadening the perspective of what constitutes an informed citizen could be beneficial in overcoming some of the barriers to inclusive communication (Aliska *et al*., 2025). Vulnerable groups are traditionally understood to be the groups directly impacted by a risk or crisis (Wisner *et al*., 2003). They also include those facing a disproportionate amount of risk due to historical, social, economic and political conditions (Campbell *et al.*, 2020), as well as due to physical, cognitive or emotional factors (Grohma *et al*., 2024). An informed citizen in this broader sense would then be someone who also has the capability to make informed choices despite communication barriers due to disadvantaged physical, socioeconomic, cognitive or emotional conditions.

Digital literacy and citizens' cybersecurity awareness

Digital literacy is by the American Library Association (ALA) defined as "the ability to use information and communication technologies to find, evaluate, create, and communicate information, requiring both cognitive and technical skills" (ALA, 2025). However, in its broadest sense, digital literacy, based on Gilster (1997) and further by Bawden (2008), is understood more as a life skill with an underpinning of critical understanding rather than a mere collection of skills and competencies. To describe the ability to recognize, interpret and evaluate differing types of data.

The digital literacy of the citizens is here relevant to understand the challenges for municipalities in using risk communication to raise awareness of information and cybersecurity risks. One such challenge, associated with the vulnerable groups described in the section above, is that cybersecurity awareness is influenced by social and digital disparities (Robinson *et al.*, 2015). Information Security Awareness is here defined as the "[. . .] overall knowledge and understanding of potential information-security-related issues and their ramifications, and what needs to be done in order to deal with security-related issues" (Bulgurcu *et al.*, 2009). Here, the knowledge gap (Fischhoff, 1995) to fill through the use of risk communication would then be the knowledge awareness of the information and cybersecurity threats. This while the "how-to-" knowledge (see Rogers, 2003) would be about what the citizen is expected to do to be able to protect themselves from harm.

There is therefore major value in municipalities taking the citizen perspective into consideration when tackling cybersecurity. Not least because the way in which an organisation approaches crisis communication and interacts with society mutually shape each other (Treurniet *et al.*, 2015). Risk communication can increase citizens' awareness of risks and their motivation to deal with them. Aware citizens have a greater capacity to receive crisis communications and manage crises (Backman, 2021). In contrast to crisis communication, risk communication can be beneficially planned, but it is dependent on how cybersecurity and communication of risks are organised in the municipality.

Research into professional norms in risk analysis and communication

Obstacles to cyber risk communication

An obstacle for cyber risk communication identified within the municipal organisation is that the knowledge gap between IT-experts and generalists at the local level is greater than at the national level (Caruson *et al.*, 2012). There is also a lack of practical experience in implementing cybersecurity policies due to resource shortages, ambiguous delineation of responsibilities and inadequate training (Norris *et al.*, 2023). Another obstacle is that there might be resistance within the organisation to changes in working methods or organisational changes (Bouckenooghe *et al.*, 2021), as well as not wanting to lose anything of value in the change process (Kotter and Schlesinger (1979/[2008]).

Tension between different professions' expectations and interests

Several professions are involved in municipalities' risk communication (Sataøen *et al*., 2024). In practice, collaborations take place between different types of experts and officials within the

organisation, such as preparedness-/security coordinators and communicators. The processes surrounding practical implementation are strongly influenced by the tension between different expectations and interests that are embedded in institutional frameworks and norms (Cedergren *et al.*, 2019). With few exceptions, there is limited understanding of these internal mechanisms within the public sector at the local level. The results of studies on risk communication at the municipal level are presented below.

What we know of risk communication at the municipal level

Municipalities can increase citizens' awareness of cybersecurity risks by communicating what the risks are. An initial obstacle is that risk communication at the local level is not planned but takes place reactively (Graham *et al.*, 2015; Sutton *et al.*, 2015; Mitcham *et al.*, 2016; Avery and Park, 2019; Fan *et al.*, 2021). A second obstacle constitutes uncertainty about what risk communication is. And the fact that in practice the boundary between risk- and crisis communication is blurred (Reynolds and Seeger, 2005; Sataøen *et al.*, 2024), limiting the municipality's ability to use effective communication strategies (Sataøen *et al.*, 2024). There is also a general lack of information on municipal websites about local risks (MSB, 2019b), which means that citizens seeking to become more aware must search for information elsewhere. The third obstacle is the tensions that can arise in the practical implementation of security work and communication (Rabe *et al.*, 2024). With communicators dependent on the risk assessments of security managers/preparedness coordinators, and the latter are not themselves aware of their influence on external risk communication (Rabe *et al.*, 2024). Furthermore, there is often no mandate from the municipal leadership to provide information about risks (Sataøen *et al.*, 2024; Rabe *et al.*, 2024). The goals and routes to legitimacy also differ between professions (Rabe *et al.*, 2024). The source of legitimacy for security managers/preparedness coordinators is security and resilience, while the legitimacy of communicators is sought among citizens through transparency and inclusion (Rabe *et al.*, 2024).

Conditions of communicating cyber risk

Addressing cybersecurity risks constitutes a significant capacity challenge for municipalities (Norris *et al.*, 2022; Hossain *et al.*, 2025). From a public administration capacity perspective, the protection of information and information systems depends on a combination of analytical capacity (such as systematic risk assessment and information classification), technological capacity (including the implementation and maintenance of appropriate and up-to-date technical safeguards) and human resources (notably the training, motivation and retention of qualified personnel) (Norris *et al.*, 2022). These functions further require coordination and integration into broader organisational planning and strategic objectives (Norris *et al.*, 2022; Wirtz and Weyerer, 2017). While technological expertise is a necessary condition for effective cybersecurity, such expertise is often difficult to recruit and sustain within the public sector (Hossain *et al.*, 2025). However, cybersecurity is not a purely technical challenge, but a socio-technical governance challenge that involves security culture, user behaviour and cognitive understandings of risk (Frandell and Feeney, 2022). Given limited resources, political leaders must prioritize the security of information system alongside other public concerns that often receive stronger recognition from the electorate (Boin *et al.*, 2017; Hossain *et al.*, 2025; Wirtz and Weyerer, 2017). Under these conditions, management and communication of cyber risks is not a straightforward task, potentially neglected by municipalities.

Even though municipalities have cybersecurity policies, if they have no practical experience of implementing them in their daily operations, local authorities cannot establish preparedness (Norris *et al.*, 2023). Other obstacles highlighted are a lack of support from the leadership (Norris *et al.*, 2023). Swedish and Norwegian municipalities do not have procedures and guidelines in place for risk communication (Sataøen *et al.*, 2024). And a lack of knowledge among officials and experts about what risk communication is (Reynolds and Seeger, 2005; Sataøen *et al.*, 2024). Questions about working procedures are therefore also intended to address what communication is like with the leadership (whether the political leadership is kept regularly informed) and

between officials (ensuring employee awareness). The staff need to have some knowledge about risks, as there is a need to select what should be communicated internally and externally. Established working procedures for communication and risk analysis are thus understood here as a kind of *prerequisite* for communication with residents. For example, to be able to communicate risks to residents, working procedures are first necessary in order to communicate/notify (internally) the leadership of information and cybersecurity issues. If such capacity is lacking, it seems unlikely that resources or tools will be available to communicate risks to residents. Furthermore, to be able to communicate risks to residents, municipalities need working procedures to classify their information and manage information and cybersecurity risks. If these procedures are not in place, it is difficult to communicate the risks.

Additionally, to be able to raise the risk awareness of residents, methods are first needed to raise that of employees. This is because the knowledge gap between IT-experts and generalists at the local level is greater than at the national level (Caruson *et al.*, 2012). Effective risk communication requires a capacity for both risk analysis and communication: an analysis of risks is communicated. Our analysis, therefore, takes an interest in established working procedures for managing cybersecurity risks, analysed in two steps. First, by analysing the dimensions that a set of established working procedures entail in municipalities. And then analysing the independent effect of the established working procedures on the extent to which municipalities are engaged in increasing residents' awareness of information and cybersecurity.

Methods

The Swedish case

In Sweden, responsibility for communicating risks, including information security and cybersecurity, is shared across municipal, county and national levels, with the Swedish Civil Defence and Resilience Agency (MCF), formerly the Swedish Civil Contingencies Agency (MSB changed its name 1 January 2026), coordinating multi-level governance. MCF provides guidelines and methodological support for RVAs, and, in collaboration with municipalities, county councils and other agencies, produces national risk assessments. The role of the MCF is also to support Sweden's national societal information security and set national strategies, action plans and regulations for cybersecurity (see SOU, 2024:18).

Legal responsibilities for crisis preparedness and risk communication

Legal responsibilities for crisis preparedness and risk communication are primarily set out in the Emergency Preparedness Ordinance SFS 2022:524, with Act 2006:544 and Ordinance SFS 2006:637 covering municipalities and regions. This legislation mandates Swedish municipalities to carry out systematic RVAs, initiate risk communication activities and ensure risk information is accessible and comprehensible to a range of vulnerable groups. While national authorities are in possession of adequate general information about risks, specifically local communication is crucial for citizens and their basis for preparedness. Swedish municipalities are also expected to raise awareness and educate citizens about, for example, cybersecurity threats and how to protect themselves (MSB, 2019a). This includes promoting digital hygiene, safe online behaviour and preparedness for cyber incidents (MSB, 2019a).

Legal responsibilities for information and cybersecurity

In terms of responsibilities related to information and cybersecurity, they are laid out in paragraphs 13§-14§ on information security and reporting of IT incidents and 26§-27§ on authorisation in Ordinance SFS 2022:524. §13 requires each government agency to ensure its information management systems meet specific, basic security requirements. §14 requires prompt reporting of IT incidents to MSB when incidents may affect information management security. §§26–27 authorise MSB to issue further regulations pertaining to security requirements and incident reporting.

For municipalities, Ordinance 2006:637 mandates systematic information security work, integration of information security into management and adherence to MCF (formerly MSB) rules for reporting of IT incidents. MSBFS 2015:5 requires municipalities to identify information of national importance and analyse information security risks in their RVAs.

Data

A cross-sectional total selection survey was employed to answer the explorative research question. Data, measurements and statistical analysis are described in the following paragraphs.

Data for this study were derived from a survey sent to all of Sweden's 290 municipalities in 2023 (10/3–25/4). The survey was administered by the Swedish Association of Local Authorities and Regions (SALAR), which represents all of Sweden's municipalities and regions. 256 municipalities responded (88%), with response rates for the variables between 212 (73%) and 234 (81%).

Measurements

Work on raising citizens' awareness of information and cybersecurity (dependent variable)

Measuring the extent to which the municipality has a citizen perspective (Johansson *et al.*, 2023; Odén *et al.*, 2016) in their information and cybersecurity work is relevant because of the following stated in ordinance SFS 2006:637. These concerning measures are taken by municipalities and regions in preparation for and during extraordinary events in peacetime and heightened preparedness. Here, the municipality has a responsibility to communicate risks to a range of pertinent actors. This includes ensuring that citizens' needs are met and that municipalities possess trustworthy and relevant information to evaluate risks, mitigate vulnerability and enhance municipalities' resilience and citizens' capabilities (Rabe *et al.*, 2024).

When asking municipalities about their efforts to protect digital information, information systems and their users – i.e. cybersecurity as defined here – we encounter a terminological challenge. Should we speak of "information security" or "cybersecurity"? Although the two concepts are analytically distinct (Taherdoost, 2022), they substantially overlap in practice. Given society's extensive reliance on digital information and information systems, the practices of information security and cybersecurity have become increasingly intertwined. For most contemporary organisations, protecting information primarily entails protecting *digital* information, which effectively makes information security a matter of cybersecurity. Reflecting this development, Moustafa *et al.* (2021) argue that in many contexts, information security has been subsumed under the broader and more widely used term cybersecurity.

Nonetheless, despite the growing emphasis on digital information (which would favour the use of "cybersecurity"), public organisations are not always quick to adopt new terminology. Instead, they often remain tied to the more traditional term *information security*, especially in policy contexts. Practitioners in municipalities are therefore more accustomed to this established vocabulary, whereas cybersecurity is newer and less precisely defined. For this reason, our survey employs the term "information security", a concept that is in principle broader, yet in practice substantially overlaps with cybersecurity. This conceptual convergence is also reflected in official guidance: for instance, when the Swedish Civil Defence and Resilience Agency (formerly MSB) (MCF, 2026b) provides recommendations to municipalities on *cybersecurity*, these draw directly on its longstanding guidance on *information security*. Moreover, the compound formulation "cyber- and information security" used throughout by MFC, signals the conceptual convergence of the two terms.

To measure this citizen perspective, we asked: "Municipalities can work to increase their residents' awareness of information security to a varying extent. To what extent is your municipality engaged in the following issues?". The first was: "Increase the municipal residents' awareness of information security". The scale for answers was: "Not at all", "To a very low degree", "To a rather low degree", "Neither nor", "To a rather high degree", "To a very high degree" and "Cannot decide".

In answering this study's explorative research question, we report and discuss the frequencies of the responses to this question. However, to further analyse, contextualise and explain the extent to which municipalities are engaged in increasing municipal residents' awareness of information security risks, we assumed the following. The variable is interpreted as a continuous dependent variable in relation to a set of explanatory variables within the realm of a set of established working procedures, as presented in the next section.

Established working procedures (independent variables)

To gauge the extent to which the municipality works with cybersecurity in various ways, we asked ten different questions about the municipality's established working procedures in relation to information security.

The survey asked municipalities ten questions with the aim of capturing the level of progress in the implementation of key activities for information security. The questions were based on the international standard for systematic information security management (ISO 27000). And on questions about working methods developed by SALAR in collaboration with the MCF's(formerly MSB's) methodological support for organisations. The questions asked was: "In the following areas, does your municipality have, or is it planning to introduce, an established working procedure so that . . .": " . . . the *political* leadership is regularly informed about information security risks"; " . . . the *administrative leadership* is regularly informed about information security risks"; ". . . information security *incidents are managed*?"; ". . . the *information assets are classified*?"; ". . . *continuity* of operations is ensured?"; ". . . employees' information security *awareness* is ensured?"; ". . . information security requirements are set in relevant *procurements*?"; " . . . the municipal information security *policy* is determined?"; ". . . the application of common working methods in the area of information security (e.g. self-monitoring, supplier follow-up) is *followed up*?"; ". . . information security *risks are managed*?".

For each of these activities, the answers were: "No", "Yes, just started", "Yes, partly established", "Yes, fully established", "Yes, but cannot determine level of establishment" and "Do not know" (for a similar scale see Karabacak *et al.*, 2016; Niazi *et al.*, 2020). These answers are interpreted as continuous variables, ranging from low to high. As the results will show, in most cases, the extent that municipalities are engaged in the work of informing citizens of information security risks is low. Therefore, the analysis tests for correlations between lower levels of progress of information security activities and lower levels of activities to inform citizens of information security risks. In the factor and regression analysis, the scales are therefore mirrored, ranging from high to low. The internal consistency for the ten items measured, Cronbach's $\alpha = 0.845$, is interpreted as sufficiently correlated, or robust, to infer that they are all measuring the same underlying construct of established working procedures.

Control variables

A control was conducted for the municipality's character and size, but the correlations are not statistically significant.

A question was asked identifying the role of the respondent: "Who or which has answered this survey?". With the answers: "information security coordinators, CISO or equivalent"; "IT managers, security managers, security coordinators, security strategists, preparedness coordinators or equivalent"; "registrars, archivists, office secretaries or equivalent" and "Other office personal, state which". The last option required an open-ended answer. The results are presented here as they are relevant for the conclusions and practical implications of this study. 84% of the municipalities are engaged in security issues. 54% of the respondents are information security coordinators, CISO or equivalent and 30% are IT-managers/security managers, security coordinators, security strategists, preparedness coordinators or equivalent. 16% consist of other administrative staff such as registrars, archivists, office secretaries, digitisation coordinators, office managers, municipal directors, etc.

Statistical analysis and ethical and data availability statements

IBM SPSS 29.0.0 was used for statistical analyses. Principal Component Analysis was used as an exploratory tool for data analysis. This is to reduce the dimensions of the variables for the information security activities and extract a smaller number of principal components (PC) according to the eigenvalue >1.0. Eigenvalues close to zero imply there is multicollinearity between items. Since the eigenvalues are well above zero, this is interpreted as a good sign, signifying a low multicollinearity between the items.

By generating a Normal Probability Plot (see Appendix 1), we checked for the normality assumption for residuals. In the plot, the points roughly follow the diagonal line, which is interpreted as following normality. To help assess the fit of the regression model (see Table 3), we plotted a residual (observed values vs. predicted values) (see Appendix 1). In looking for patterns, there seems to be one outlier far from the line, no U-shapes, curves or shapes where variance changes. The Variance Inflation Factor (VIF) was used to detect multicollinearity in the regression (see Table 3). Since the values are above 1 and below 5, this is interpreted as a moderate correlation.

Data is available from the corresponding author upon reasonable request, and the study has been reviewed and approved by the Swedish Ethical Review Authority (2023-02308-01).

Results

Low level of municipal engagement in raising citizens' awareness

The question of the extent to which municipalities are engaged in work to increase residents' awareness of information security is answered initially below. The dimensions that the municipalities' established working procedures entail are subsequently analysed.

The study's results show the following. That the majority of Sweden's municipalities (81%) state that they work to a rather (23%) or very low (29%) degree, or not at all (29%), to enhance residents' awareness of information security (Table 1). Meanwhile, 16% are uncertain, i.e. they state that they work to neither a low nor a high degree, or that they are not able to assess it. Only a minor proportion, 3%, of the municipalities state that they are working to a rather high degree to increase residents' awareness of information security risks. No municipality states that they are working to a very high degree on the issue.

Implementation of established working routines

The established working procedures asked for concern about the existence of established routines in the organisation to perform a task. So that the task is handled in a similar way over time and regardless of who performs the task. In information security work, municipalities have established certain types of routines, while others have not. Among those who have introduced the routines, the implementation of these varies.

Table 1. Proportion of municipalities engaged in raising citizens' awareness of information security 2023 (per cent)

	Total proportion
To a very high degree	0
To a rather high degree	3
Neither nor or cannot decide	16
To a rather low degree	23
To a very low degree	29
Not at all	29
Total proportion	100
Total municipalities	234

As presented in Table 2, two PCs were extracted from the PCA approach with the eigenvalue >1.0. PC1 with positive and strong loading due to the principal established procedures for Information security risks (0.743) and incidents (0.713) being managed, and PC1 explaining 44.2% of the total variance. PC2 with a negative and strong loading primarily due to the established procedures of the political (−0.551) and administrative leadership (−0.484) being informed on a regular basis. PC2 explained 11.2% of the total variance. Together the two PCs explain 55.3% of the variation, which is interpreted as reasonably valid.

Two dimensions in established working procedures

How should we then understand these two principal components in how municipalities responded to the questions regarding established working procedures (Table 2)? One way to understand them is as two distinct dimensions. Here, the working procedures of securing the active involvement of top management, both the political leadership and the operational

Table 2. Two dimensions in the municipalities' established procedures for information security

Established procedures for information security	Component 1	2
Information security risks are managed	0.743	−0.100
Information security incidents are managed	0.713	0.019
Continuity of operations is ensured	0.698	0.244
Information security requirements are set in relevant procurements	0.664	0.239
The information assets are classified	0.637	0.484
Employees' information security awareness is ensured	0.633	0.082
The municipal information security policy is in place	0.580	0.382
The political leadership is informed about information security risks	0.642	−0.551
The administrative leadership is informed about information security risks	0.695	−0.484
The application of working methods in information security is followed up	0.652	−0.239
Eigenvalues	4.425	1.110
% of Variance	44.253	11.095
Cumulative %	44.253	55.348

Note(s): Extraction method: Principal Component Analysis

Table 3. Independent effects of established procedures for information security in Swedish municipalities on their work to raise citizens' awareness of information security 2023 (standardised regression coefficient, b-value and significance, *p*-value, VIF)

Established working procedures	*b*-value and *p*-value	VIF
The political leadership is regularly informed about information security risks	+0.34***	1.81
Information security risks are managed	+0.24**	2.01
Administrative leadership is regularly informed about information security risks	−0.19*	1.97
The application of working methods in information security is followed up	+0.16	1.62
The information assets are classified	−0.08	1.61
Continuity of operations is ensured	−0.08	1.65
The municipal information security policy is in place	+0.06	1.39
Information security requirements are set in relevant procurements	+0.06	1.54
Employees' information security awareness is ensured	+0.05	1.43
Information security incidents are managed	−0.04	1.70
Adjusted R^2	0.19	
Number of municipalities	234	

Note(s): Bivariate correlation (stand. B-value). *$p < 0.05$; **$p < 0.01$; ***$p < 0.001$. $N = 234$

administrative leadership, would be one of these dimensions. This together with following up working methods in information security. Here, called *Political Governance*, in terms of facilitating means for the political leadership to be actively involved in asserting influence on the municipal information security management. On the other hand, the second dimension, here called *Continuity in Operations*, ensures that information security risks and incidents are managed operationally and that information assets are classified. As well as that there is more passive managerial involvement, information security policy is in place, and there is continuity of operations. As well as that information security requirements are set in relevant procurements and employees are aware of information security.

Relationship between engagement and established working routines

Since the majority of Swedish municipalities are not engaged in increasing residents' awareness of information security risks, the following results will endeavour to understand and reason about why this is the case. And, what challenges it may entail. The relationships initially sought here are between how a *lower* degree of established working procedures correlates with a *lower* degree of work to increase residents' awareness of information security risks.

Multiple linear regression analysis was used to identify factors associated with Swedish municipalities' lower work to raise citizens' awareness of information security. The model used does not test all the plausible factors in the literature presented in this paper. Due to the explorative nature of the study, the model tested focuses on the level of implementation of established working procedures. The analysis in this section shows that the level of implementation of established working procedures explained 19% of the changes in the dependent variable (adjusted $R^2 = 0.19$) (Table 3). That is, the level of municipalities' work to raise citizens' awareness of information security.

The multicollinearity in the regression analysis is moderate, meaning that the level of implementation of established working procedures as a whole is what best can explain the changes in the dependent variable. With that in mind, the following independent effects of three of the variables should not be overstated, but looked upon as indications. Among the variables included in the model, the lower levels of keeping the political leadership regularly informed about information security risks (b = + 0.34***), were significantly correlated with the *lower levels* of work to raise citizens' awareness of information security. And the lower levels of managing information security risks (b = + 0.24**). This is in contradiction to the lower levels of keeping the administrative leadership regularly informed about information security risks (b = − 0.19**). Those were significantly correlated with the *higher levels* of work to raise citizens' awareness of information security (Table 3).

These observations provide tentative support for the idea that certain internal working procedures in cybersecurity are prerequisites for effective communication with residents about cyber risks. First, the ability to communicate risks externally presupposes established routines for internal communication with municipal leadership; without such a capacity for internal communication, external communication is unlikely to develop. Second, communicating risks to citizens requires systematic knowledge of the risks themselves. In other words, municipalities must have procedures in place to manage information and cybersecurity risks before they can convey these risks to the public. In particular, our findings indicate two factors as important for taking steps towards a citizen perspective in municipal cybersecurity. The capacity for internal communication with political leadership and the capacity for systematic risk analysis.

Discussion and conclusions

The purpose of the article was to analyse the extent to which municipalities are engaged in increasing citizens' awareness of information and cybersecurity risks and to discuss why potential challenges might arise. Since, as far as we can tell, no previous research has been conducted into the citizen perspective in relation to work on information and cybersecurity

risks at the municipal level. The article's contribution is to show that municipalities are not engaged to any major extent in increasing residents' awareness of information and cybersecurity. This implies that the citizen perspective is not prominent in the work that municipalities carry out in relation to information and cybersecurity risks (Johansson *et al.*, 2023; Odén *et al.*, 2016).

In the discussion of why this is the case, based on the empirical findings in this study, we address the role of internal working procedures for information and cybersecurity that are established in municipalities. Municipalities with a higher capacity for internal communication with political leadership and the capacity for systematic risk analysis tend to engage more in communication of cyber risks to citizens.

Moreover, the discussion of why we find low levels of engagement in communicating cyber risk to citizens can be further understood by the interpretive insights from previous literature. In the literature that emphasize the citizens' increased demands for openness, transparency and accountability from authorities (Macmanus *et al.*, 2012). Earlier studies from the USA (Macmanus *et al.*, 2012), which are somewhat dated, highlight the explanation that there is a contradiction between two perspectives – transparency and integrity. The contradiction between the two perspectives is what we have chosen to call the cybersecurity paradox. The contradiction can be seen as a general way to understand why municipalities do not develop a more comprehensive capacity to protect citizens from a range of cyber threats. Norris *et al.* (2023: 652) have further highlighted the incapacity of local authorities to manage cybersecurity. This has been explained by insufficient funding and insufficient human resources to achieve sufficient cybersecurity (Norris *et al.*, 2023). The connection between social (weather and perceptions) and technical factors (networks, capacity, technical infrastructure) and the capacity to manage cyber incidents has also been previously highlighted in the literature (Frandell and Feeney, 2022, pp. 559–560). What is generally considered in this article, i.e. what role local authorities should play and where the boundaries should be for their responsibility towards citizens, is a central and urgent issue. This contrasts with the authorities' requirement to protect sensitive information (Frandell and Feeney, 2022; Caldarulo *et al.*, 2022).

Lack of established working procedures

The first challenge is based on the results of this study, which show the relevance of the model with implemented established working procedures to raise citizens' awareness of information and cybersecurity risks. Here, the model used explained 19% of the changes in the level of municipalities' work to raise citizens' awareness of information and cybersecurity risks.

A previous study identified the lack of implementation of cybersecurity policies in everyday operations as an obstacle (Norris *et al.*, 2023). Another study found that there are no routines and guidelines in place for risk communication and that officials and experts were unsure of what risk communication was and how it differed from crisis communication (Sataøen *et al.*, 2024). The empirical findings in this article are that the municipalities rarely engage in raising residents' awareness of cybersecurity risks, and that the model with established working procedures is relevant to understand why. Through interpretive insights from the previous literature mentioned above, the lack of municipal engagement could be related to the municipality's lack of implementation of cybersecurity policies. Which may involve a lack of routines and guidelines for how cybersecurity should be communicated. Our findings, therefore, suggest that effective communication of cyber risk requires a capacity for both risk analysis and communication. An analysis of the risks to be communicated, as well as how to do so.

Security trumps transparency

Based on interpretive insights from the previous literature the second challenge concerns how security personnel work in relation to risk management in municipalities. Previous research

suggests that there are strong professional norms in municipalities, where security personnel prioritise confidentiality over transparency (Sataøen *et al.*, 2024; Rabe *et al.*, 2024). It also appears that security personnel constitute the dominant professional group in municipal risk management. They have access to the information and have the highest status in relation to the process (Sataøen *et al.*, 2024; Rabe *et al.*, 2024). It appears that security personnel are simultaneously unaware of their dominant position (Rabe *et al.*, 2024). Based on these interpretive insights from the previous literature, a plausible understanding of why municipalities rarely consider the citizen perspective in cybersecurity work, is the following. The personnel responsible for cybersecurity in prioritising security over transparency, rarely have the citizen perspective on their agenda. However, acknowledging the relevance of transparency here is relevant in understanding why risk communication is important in the municipality's work on cybersecurity (Sellnow and Seeger, 2013). This is because previous literature claim that transparency can affect the individual's future and reduce the risk of adverse consequences (Sellnow and Seeger, 2013). Which can include engaged citizens seeking knowledge elsewhere in order to be better prepared in the event of a crisis (MSB, 2019a).

Cybersecurity paradox

Based on the insights from previous research, we suggest that the tension between, on the one hand, the demand for transparency and openness. And, on the other hand, security and confidentiality are reinforced by the fact that the task is divided between different officials (Rabe *et al.*, 2024). Previous research has shown that the security personnel differ from the communicators in that they have a technical view of risks. Further, they use hierarchical and one-way communication with the communicators (Rabe *et al.*, 2024). According to previous research, there may also be a resistance to change because one party risks losing something of value (Kotter and Schlesinger, 1979/[2008]). In the study by Rabe *et al.* (2024), it appears that security personnel have a high status. And that risk management in the municipality is mainly conducted by security personnel, implying that the communicators are not involved and cannot provide information about risks. Based on these interpretive insights from the previous literature, a plausible understanding of why challenges arise can be found in the locking of positions described. The dilemma of citizens' demands to "open up", and the possibilities for accountability, and to "lock down" and protect integrity-sensitive data, are reinforced. This is then interpreted to be due to a major confidentiality norm that is in place. That security is a higher priority, and status provides little incentive for change. Neither do the security personnel perceive the problem, with the communicators appearing to be a hidden resource for supplying the municipality's residents with information about cybersecurity.

Study limitations

This study has two limitations. The first is that the survey was targeted at the municipality as an organisation, with the result that the same professions responsible for security and preparedness have not consistently answered the survey. The second is that the results may make it difficult to perceive the extent to which municipalities are engaged in increasing residents' awareness of cybersecurity in the municipal sector as a whole.

Practical implications and conclusions

The study has three practical implications. The first is that despite Sweden having optimum conditions for transparency in the public realm and good conditions for communicating risks, the communicating cyber risk with citizens is given low priority. Municipalities do not make plans for risk communication, neither specifically for information and cybersecurity risks nor for risks in general. The study shows that municipalities are not putting work into increasing residents' awareness of information and cybersecurity risks. There is a lack of established

working procedures for dealing with this issue. The results of the study can be used to increase municipalities' awareness of the issue by highlighting its negligence.

The second implication is that there are low incentives for cooperation between security personnel and communicators. To raise citizen awareness, this collaboration most likely needs to be improved. Both professions have crucial roles in communicating cyber risks to citizens. Security personnel need to assess the risks and the confidentiality of content. Communicators need to be involved in the strategic planning of risk communication. Through better collaboration between security personnel and communicators, the cybersecurity paradox can be mitigated. Established forms of collaboration between these two competencies can be a good asset for a municipality when an incident occurs.

Thirdly, municipalities need to find an optimal use of internal and external communication, while at the same time not spreading sensitive information to unauthorized parties. This study highlights this dilemma, which in a critical situation can have major consequences in the event of an information or cybersecurity incident.

The recommendation to overcome the consequences of a cybersecurity paradox is then the following. To more effectively address residents' awareness of information security and cybersecurity, a shift in political will is required. Cybersecurity must attain a more prominent position on the local political agenda, likely accompanied by increased resource allocation. This process also presupposes enhanced capacity to translate and mediate complex technical aspects of cybersecurity for non-technical audiences, including elected officials and top management. Such changes, however, are not easily achieved. Nevertheless, with upcoming directives in the European Union aimed at strengthening regulatory requirements for cybersecurity (NIS 2) are likely to elevate attention to and investment in cybersecurity governance are expected to grow. These capacity-building efforts may also produce spillover effects, strengthening municipalities' ability to engage with and enhance cybersecurity awareness among citizens.

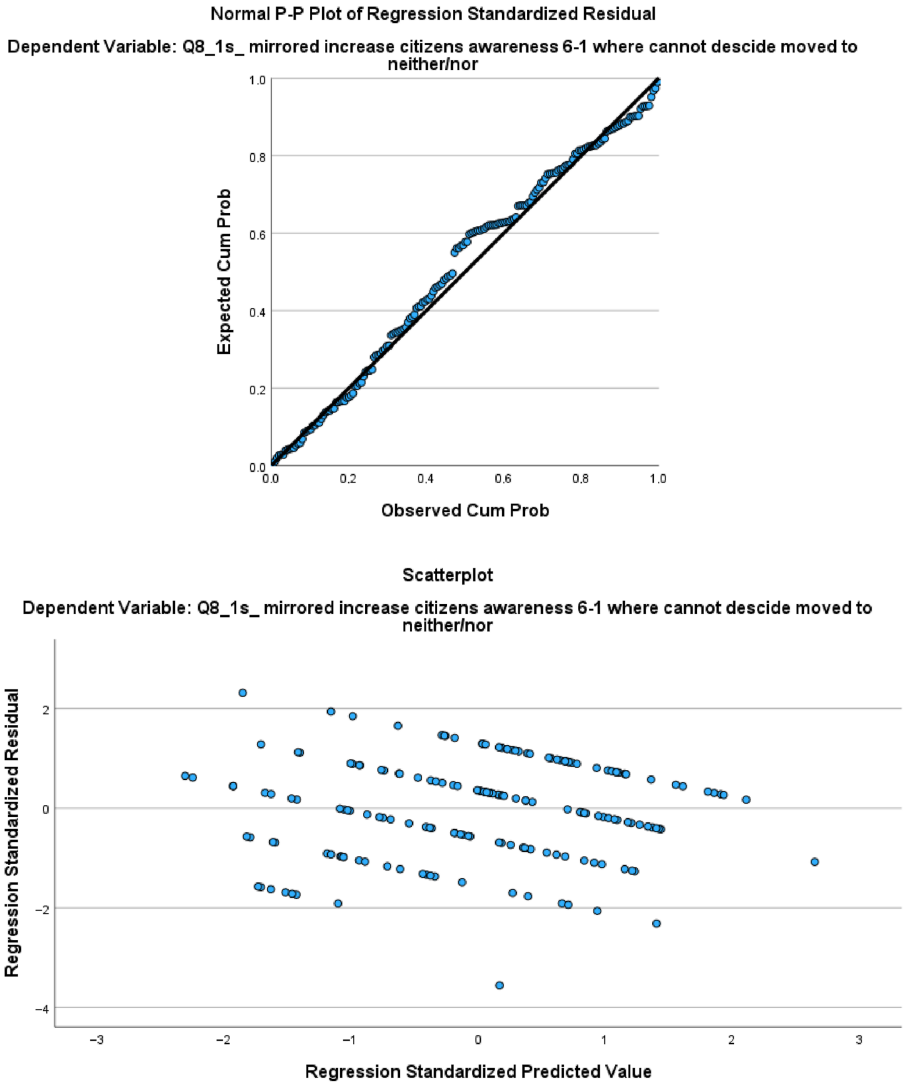
To encourage cooperation between security personnel and communicators one way ahead would be to strive for a municipal decision to produce a public version of the RVA. This would neither threaten the legitimacy of the security personnel nor the legitimacy of the communicators. In this way the political leadership in the municipality is kept informed, as well as ensuring the early involvement of the communicators in the process. This could ensure that the extensive and security-classified information in the RVAs could remain secure. What could be said officially and communicated to residents would also be accessible, as well as potentially raising citizens' awareness of cybersecurity risks.

Acknowledgments

The authors thank the municipalities that participated in the cybersecurity survey conducted in collaboration with the Swedish Association of Local Authorities and Regions (SALAR). In particular, the authors would like to express our appreciation to Jonas Nilsson, Information Security Manager at the Swedish Association of Local Authorities and Regions, for his valuable cooperation in the design of the survey. Finally, the authors thank the Editor-in-Chief, the Associate Editor, and the two anonymous reviewers for their constructive and insightful comments.

(The Appendix follows overleaf)

Appendix



Notes

1. In broad terms, cybersecurity refers to the protection of digital information and information systems, as well as their users, from cyber threats. Narrower definitions restrict "cyber threats" to antagonistic actions (von Solms and van Niekerk, 2013), while others adopt a broader view (ENISA, 2015). Although cyberattacks are undeniably central, we define cyber threats as any potential danger to digital data, systems or users. This inclusive approach reflects the context of our study, which examines public organisations in Sweden, where protective initiatives are not always differentiated by the intentionality of the threat. For instance, the Civil Defence and Resilience Agency (MCF, 2026a) - a central actor in coordinating and supporting public sector cybersecurity – defines cyber threats as

including not only hostile actions but also human error, system malfunctions and natural events such as storms or earthquakes. Related to this is the distinction between cybersecurity and information security (Taherdoost, 2022), the latter of which, i.e. the older concept, is typically defined in terms of confidentiality, integrity and availability of information (Lundgren and Möller, 2019). While information security encompasses both digital and non-digital domains, the growing centrality of digitalisation means that protection of digital information has become a main concern, thereby overlapping with cybersecurity. Consequently, although cybersecurity and information security are distinct in principle, in practice, management of them within the public sector is substantially convergent. Today, information security is to a large extent – though not entirely – addressed through cybersecurity measures, as defined here (Moustafa *et al*., 2021).

References

ALA (2025), "The American library association", available at: https://www.ala.org/ala-literacy-clearinghouse.Downloaded2025-12-18

Aliska, I., Knudsen, S., Mehdi, Z. and Anson, S. (2025), "Inclusivity through co-creation: insights for practitioners to engage vulnerable populations in risk communication development", *International Journal of Disaster Risk Reduction*, Vol. 118, 105214, doi: 10.1016/j.ijdrr.2025.105214.

Andreasson, A., Artman, H., Brynielsson, J. and Franke, U. (2024), "Cybersecurity work at Swedish administrative authorities: taking action or waiting for approval", *Cognition, Technology and Work*, Vol. 26 No. 4, pp. 709-731, doi: 10.1007/s10111-024-00779-1.

Avery, E.J. and Park, S. (2019), "The influences of relationship quality with external partners and required levels of approval of messaging on crisis preparedness", *Public Relations Review*, Vol. 45 No. 1, pp. 119-127, doi: 10.1016/j.pubrev.2018.08.001.

Backman, S. (2021), "Conceptualizing cyber crises", *Journal of Contingencies and Crisis Management*, Vol. 29 No. 4, pp. 429-438, doi: 10.1111/1468-5973.12347.

Bawden, D. (2008), "Origins and concepts of digital literacy", in Lankshear, C. and Knobel, M. (Eds), *Digital Literacies: Concepts, Policies and Practices*, Peter Lang Publishing, pp. 17-32.

Boholm, Å. (2019), "Risk communication as government agency organizational practice", *Risk Analysis*, Vol. 39 No. 8, pp. 1695-1706, doi: 10.1111/risa.13302.

Boin, A., Hart, P., Stern, E. and Sundelius, B. (2017), *The Politics of Crisis Management*, Cambridge University Press, Cambridge.

Bouckenooghe, D., Schwarz, G.M., Kanar, A. and Sanders, K. (2021), "Revisiting research on attitudes toward organizational change: bibliometric analysis and content facet analysis", *Journal of Business Research*, Vol. 135, pp. 137-148, doi: 10.1016/j.jbusres.2021.06.028.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2009), "Roles of information security awareness and perceived fairness in information security policy compliance", *AMCIS 2009 Proceedings*, p. 419, Downloaded 2025-12-18.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010), "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness", *MIS Quarterly*, Vol. 34 No. 3, pp. 523-548, doi: 10.2307/25750690.

Caldarulo, M., Welch, E.W. and Feeney, M.K. (2022), "Determinants of cyber-incidents among small and medium US cities", *Government Information Quarterly*, Vol. 39 No. 3, pp. 1-12, doi: 10.1016/j.giq.2022.101703.

Caldarulo, M., Olsen, J. and Feeney, M.K. (2024), "Oversharing: the downside of data sharing in local government", *Public Administration*, Vol. 102 No. 4, pp. 1647-1664, doi: 10.1111/padm.12993.

Campbell, N., Roper-Fetter, K. and Yoder, M. (2020), *Risk Communication Involving Vulnerable Populations: An Annotated Bibliography*, Natural Hazards Center, University of Colorado Boulder, Boulder, CO.

Caruson, K., MacManus, S.A. and McPhee, B.D. (2012), "Cybersecurity policy-making at the local government level: an analysis of threats, preparedness, and bureaucratic roadblocks to success", *Homeland Security and Emergency Management*, Vol. 9 No. 2, pp. 1-22, doi: 10.1515/jhsem-2012-0003.

Cedergren, A., Swaling, H., Vidar, H., Henrik, D., Carl, M.S., Karin, A., Anders, P.-A., Bengtsson, J. and Sparf, A. (2019), "Understanding practical challenges to risk and vulnerability assessments: the case of Swedish municipalities", *Journal of Risk Research*, Vol. 22 No. 6, pp. 782-795, doi: 10.1080/13669877.2018.1485169.

Chodakowska, A., Kańduła, S. and Przybylska, J. (2022), "Cybersecurity in the local government sector in Poland: more work needs to be done", *Lex Localis – Journal of Local Self-Government*, Vol. 29 No. 1, pp. 161-192.

Covello, V.T., von Winterfeldt, D. and Slovic, P. (1986), *Risk Communication: A Review of the Literature*, National Science Foundation, Washington, DC.

Department of defence (2006), "SFS 2006:637", *Förordning om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap*, [Ordinance on measures taken by municipalities and regions in preparation for and during extraordinary events in peacetime and heightened preparedness].

Dunn Cavelty, M. (2024), *The Politics of Cyber-Security*, Routledge, New York.

ENISA (2015), "Definition of cybersecurity: gaps and overlaps in standardisation", *The European Union Agency for Network and Information Security (ENISA)*, available at: https://www.enisa.europa.eu/sites/default/files/publications/Cybersecurity_Definition_Gaps_v1_0.pdf (accessed 15 January 2026).

Fan, C., Jiang, Y. and Mostafavi, A. (2021), "The role of local influential users in spread of situational crisis information", *Journal of Computer-Mediated Communication*, Vol. 26 No. 2, pp. 108-127, doi: 10.1093/jcmc/zmaa020.

Fischhoff, B. (1995), "Risk perception and communication unplugged: twenty years of process", *Risk Analysis*, Vol. 15 No. 2, pp. 137-145, doi: 10.1111/j.1539-6924.1995.tb00308.x.

Frandell, A. and Feeney, M. (2022), "Cybersecurity threats in local government: a sociotechnical perspective", *American Review of Public Administration*, Vol. 52 No. 8, pp. 558-572, doi: 10.1177/02750740221125432.

Fuchs, S., Birkmann, J. and Glade, T. (2012), "Vulnerability assessment in natural hazard and risk analysis: current approaches and future challenges", *Natural Hazards*, Vol. 64 No. 3, pp. 1969-1975, doi: 10.1007/s11069-012-0352-9.

Gilster, P. (1997), *Digital Literacy*, Wiley, New York.

Government (2022), "SFS 2022:524", *Förordning om statliga myndigheters beredskap*, [Emergency preparedness ordinance for state authorities].

Government (2024), "SOU 2024:18", *Nya regler om cybersäkerhet*, [New rules on cybersecurity].

Graham, M.W., Avery, E.J. and Park, S. (2015), "The role of social media in local government crisis communications", *Public Relations Review*, Vol. 41 No. 3, pp. 386-394, doi: 10.1016/j.pubrev.2015.02.001.

Grohma, P., Wojczewski, S., Juen, B., Riedel, P.-L., Seufert, F., Streifeneder, V., Reichel, S., Pichler, S., Kulcar, V., Nestlinger, S., Stickler, M., Schober, C., Scheller, H. and Kutalek, R. (2024), "Defining vulnerabilities and enabling community engagement in epidemics preparedness: the CAVE model from Austria", *European Journal of Public Health*, Vol. 35 No. 2, pp. 276-281, doi: 10.1093/eurpub/ckae173.

Hatcher, W., Meares, W.L. and Heslen, J. (2020), "The cybersecurity of municipalities in the United States: an exploratory survey of policies and practices", *Journal of Cyber Policy*, Vol. 5 No. 2, pp. 302-325, doi: 10.1080/23738871.2020.1792956.

Hood, C. and Heald, D. (2006), *Transparency. The Key to Better Governance?*, Oxford University Press, New York.

Hossain, S.T., Yigitcanlar, T., Nguyen, K. and Xu, Y. (2025), "Cybersecurity in local governments: a systematic review and framework of key challenges", *Urban Governance*, Vol. 5 No. 1, pp. 1-19.

Johansson, B., Ihlen, Ø., Lindholm, J.B.-Ø. and Mark (2023), "Communicating a pandemic in the Nordic countries", in Johansson, B., Ihlen, Ø., Lindholm, J.B.-Ø. and Mark (Eds),

Communicating a Pandemic – Crisis Management and Covid-19 in the Nordic Countries, Nordicom, Gothenburg.

Karabacak, B., Yildirim, S.O. and Baykal, N. (2016), "A vulnerability-driven cybersecurity maturity model for measuring national critical infrastructure protection preparedness", *International Journal of Critical Infrastructure Protection*, Vol. 15, pp. 47-59, doi: 10.1016/j.ijcip.2016.10.001.

Kotter, J.P. and Schlesinger, L.A. (1979), "Choosing strategies for change", *Harvard Business Review*, pp. 2-11, reprint Best of HBR July–August 2008.

Lidberg, J. (2009), "The international freedom of information index. A watchdog of transparency in practice", *Nordicom Review*, Vol. 30 No. 1, pp. 167-183, doi: 10.1515/nor-2017-0145.

Lundgren, B. and Möller, N. (2019), "Defining information security", *Science and Engineering Ethics*, Vol. 25 No. 2, pp. 419-441, doi: 10.1007/s11948-017-9992-1.

Macmanus, S., Caruson, K. and McPhee, B.D. (2012), "Cybersecurity at the local government level: balancing demands for transparency and private rights", *Journal of Urban Affairs*, Vol. 35 No. 4, pp. 451-470.

MCF [Swedish Civil Defence and Resilience Agency] (2026a), "Cyberhot", [Cyber threats], available at: https://www.mcf.se/sv/amnesomraden/informationssakerhet-och-cybersakerhet/risker-och-sarbarheter-inom-cybersakerhet-och-cyberfysiska-system/hot-och-metoder-inom-cybersakerhet/cyberhot/ (accessed 15 January 2026).

MCF [Swedish Civil Defence and Resilience Agency] (2026b), "Guide till en cybersäker kommun [guidance for a cybersecure municipality]", available at: https://www.mcf.se/contentassets/4569eeabc8e64db3952c5c6e0cbc20ae/msb-guide-till-en-cybersaker-kommun-241211.pdf (accessed 15 January 2026).

Mitcham, D., Taylor, M. and Harris, C. (2016), "Utilizing social media for information dispersal during local disasters: the communication hub framework for local emergency management", *International Journal of Environmental Research and Public Health*, Vol. 18, 10784, pp. 1-16, doi: 10.3390/ijerph182010784.

Moustafa, Ahmed, A., Bello, A. and Maurushat, A. (2021), "The role of user behaviour in improving cybersecurity management", *Frontiers in Psychology*, Vol. 12, 561011, doi: 10.3389/fpsyg.2021.561011.

MSB [Swedish Civil Contingencies Agency] (2015), "MSBFS 2015:5 Föreskrifter och allmänna råd om kommuners risk- och sårbarhetsanalyser [regulations and general advice on municipalities' risk and vulnerability analyses]".

MSB [Swedish Civil Contingencies Agency] (2019a), *Comprehensive Cyber Security Action Plan 2019-2022 – March 2019*", MSB, Karlstad.

MSB [Swedish Civil Contingencies Agency] (2019b), "Kommunala webbplatsers kommunikation om lokala risker", [Municipal websites' Communication of local risks].

Niazi, M., Saeed, A.M., Alshayeb, M., Mahmood, S. and Zafar, S. (2020), "A maturity model for secure requirements engineering", *Computers and Security*, Vol. 95, 101852, doi: 10.1016/j.cose.2020.101852.

Norris, D.F., Mateczun, L., Joshi, A. and Finin, T. (2019), "Cyberattacks at the grass roots: American local governments and the need for high levels of cybersecurity", *Public Administration Review*, Vol. 79 No. 6, pp. 895-904, doi: 10.1111/puar.13028.

Norris, D.F., Mateczun, L.K. and Forno, R.F. (2022), *Cybersecurity and Local Government*, John Wiley & Sons, Hoboken, NJ.

Norris, D.F., Mateczun, L., Hatcher, W., Meares, W.L. and Heslen, J. (2023), "Local government cyber insecurity: causes and recommendations for improvement", *Public Administration Review*, Vol. 84 No. 4, pp. 651-659, doi: 10.1111/puar.13743.

National Research Council (NRC) Committee on Risk Perception and Communication (1989), *Improving Risk Communication*, National Academy Press, Washington, DC.

Odén, T., Djerf-Pierre, M., Ghersetti, M. and Johansson, B. (2016), *Kriskommunikation 2.0 – Allmänhet, medier och myndigheter i det digitala medielandskapet*, JMG, Göteborg, Crisis Communication 2.0 – The Public, Media and Institutions in the Digital Media Landscape.

Preis, B. and Susskind, L. (2022), "Municipal cybersecurity: more work needs to be done", *Urban Affairs Review*, Vol. 58 No. 2, pp. 614-629, doi: 10.1177/1078087420973760.

Rabe, L., Sataøen, H.L., Lidskog, R. and Eriksson, M. (2024), "Making risk communication in practice: dimensions of professional logics in risk and vulnerability assessments", *Journal of Risk Research*, Vol. 27 No. 3, pp. 1-15, doi: 10.1080/13669877.2024.2328199.

Reynolds, B. and Seeger, M.W. (2005), "Crisis and emergency risk communication as an integrative model", *Journal of Health Communication*, Vol. 10 No. 1, pp. 43-55, doi: 10.1080/10810730590904571.

Roberts, A. (2006), *Blacked Out: Government Secrecy in the Information Age*, University Press, Cambridge.

Robinson, L., Cotten, S.R., Ono, H., Quan-Haase, A., Mesch, G., Chen, W., Schulz, Jeremy, H., Timothy, M. and Stern, M.J. (2015), "Digital inequalities and why they matter", *Information, Communication and Society*, Vol. 18 No. 5, pp. 569-582, doi: 10.1080/1369118x.2015.1012532.

Rogers, E.M. (2003), *Diffusion of Innovations*, 5th ed., Free Press, New York.

Sandstig, G. (2025), "Riskkommunikation vid samhälleliga cyberkriser. Arbetsrapport nr. 94", [Risk Communication in Societal Cyber Crises. Working Report no. 94]. University of Gothenburg, Department of Journalism, Media and Communication (JMG).

Sataøen, H.L., Skotenes, Ø., Ruth, H., Kåre and Eriksson, M. (2024), "Municipal risk communication challenges in the Nordic context: organizing risk ownership", *Risk, Hazards and Crisis in Public Policy*, pp. 1-20.

Sellnow, T.L. and Seeger, M.W. (2013), *Theorizing Crisis Communication*, Wiley-Blackwell, Chichester.

Sellnow, T.L., Ulmer, R.R., Seeger, M.W. and Littlefield, R.S. (2009), *Effective Risk Communication. A Message–Centered Approach*, Springer, New York.

Sutton, J., League, C., Sellnow, T.L. and Sellnow, D.D. (2015), "Terse messaging and public health in the midst of natural disasters: the case of the boulder floods", *Health Communication*, Vol. 30 No. 2, pp. 135-143, doi: 10.1080/10410236.2014.974124.

Taherdoost, H. (2022), "Cybersecurity vs. information security", *Procedia Computer Science*, Vol. 215, pp. 483-487, doi: 10.1016/j.procs.2022.12.050.

Transparency International (2024), "Annual report 2023", available at: https://files.transparencycdn.org/images/2023_TransparencyInternationalAnnualReport_EN.pdf (accessed 2 December 2026).

Treurniet, W., Messemaker, M., Jeoren, W. and Boersma, F.K. (2015), "Shaping the societal impact of emergencies: striking a balance between control and cooperation", *International Journal of Emergency Services*, Vol. 4 No. 1, pp. 129-151, doi: 10.1108/ijes-06-2014-0007.

Von Solms, R. and Niekerk, J. (2013), "From information security to cybersecurity", *Computers and Security*, Vol. 38, pp. 97-102.

Wirtz, B.W. and Weyerer, J.C. (2017), "Cyberterrorism and cyber attacks in the public sector: how public administration copes with digital threats", *International Journal of Public Administration*, Vol. 4 No. 13, pp. 1085-1100, doi: 10.1080/01900692.2016.1242614.

Wisner, B., Blaikie, P.M., Cannon, T. and Davis, I. (2003), *At Risk: Natural Hazards, People's Vulnerability and Disasters*, 2nd ed., Routledge, London.

Corresponding author
Gabriella Sandstig can be contacted at: gabriella.sandstig@jmg.gu.se